

CPNI Compliance Policies **of P.A. Dominguez, Inc.**

The following summary describes the policies of P.A. Dominguez, Inc. (the "Company") that are designed to protect the confidentiality of Customer Proprietary Network Information ("CPNI") and to assure compliance with the rules of the Federal Communications Commission ("FCC") set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq.* Company substantially revised and updated its policies and conducted new training prior to the effective date of the FCC's new rules adopted in *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22 (rel. April 2, 2007).

CPNI is "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."

The Company's policy, administered by Peter Dominguez, establishes the following parameters regarding the use and disclosure of CPNI:

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

Company will use, disclose, or permit access to CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including the publishing of directories; to initiate, render, bill and collect for communications services; to protect the rights or property of the Company, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide inside wiring installation, maintenance, or repair services; as required by law (such as pursuant to a valid request from law enforcement or a court order or other appropriate authority); or as expressly authorized by the customer.

Company does not use CPNI to market service offerings among the different categories of service, or even within the same category of service, that it provides to subscribers. Company's marketing department does not have access to customer's CPNI. Although current Company policy is not to use CPNI for marketing, in the event that any employee or agent wishes to use CPNI for marketing or to seek customer approval for such use, such proposed use is subject to a supervisory review process that shall involve a supervisor designated by the senior employee responsible for marketing and the CPNI Compliance Officer. If such use is approved, Company shall modify these policies and conduct additional training as needed to assure compliance with the FCC's rules.

Company does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

Above and beyond the specific FCC requirements, Company will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to Company's existing policies that would strengthen protection of CPNI, they should report such information immediately to Company's CPNI Compliance Officer so that Company may evaluate whether existing policies should be supplemented or changed.

A. Assignment of CPNI Passwords

Company has assigned CPNI Password for each person who has computer access to customer information. The password assigned, it is not expected to consist of any material portion of the customer's name, family names, account number, telephone number, street address, zip code, social security number, date of birth, or other biographical or account information. The CPNI Password is only used internally for company access to this information.

B. Inbound Calls to Company Requesting CPNI

Company presently does not disclose such information.

C. In-Person Disclosure of CPNI at Company Offices

Company may disclose a customer's CPNI to an authorized person visiting a Company office upon verifying that person's identity through a valid, non-expired government-issued photo ID (such as a driver's license, passport, or comparable ID) matching the customer's account information.

D. Online Access to CPNI

Company presently does not disclose such information.

E. Notice of Account Changes

Account changes are only made with direct communications with the customer.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Any Company employee that becomes aware of any breaches, suspected breaches or attempted breaches of CPNI must report such information immediately to the Company CPNI Compliance Officer, and such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

Company's CPNI Compliance Officer is Peter Dominguez, who may be contacted at 914-423-4012 or peter@pad.com

It is Company's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to our customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate the Company's CPNI compliance policies are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

A. Identifying a "Breach"

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Officer.

If a Company employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to Company's CPNI Compliance Officer who will determine whether to report the incident to law enforcement and/or take other appropriate action. Company's CPNI Compliance Officer will determine whether it is appropriate to update Company's CPNI policies or training materials in light of any new information; the FCC's rules require Company on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting."

B. Notification Procedures

As soon as practicable, and in no event later than seven (7) business days upon learning of a breach, the Company CPNI Compliance Officer shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: <https://www.cpnireporting.gov>. Company's FRN number and password may be required to submit a report. If this link is not responsive, they

should contact counsel or the FCC's Enforcement Bureau (202-418-7450 or <http://www.fcc.gov/eb/cpni>) for instructions.

Company will not under any circumstances notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided below. (A full business day does not count a business day on which the notice was provided.) Federal law requires compliance with this requirement even if state law requires disclosure. If Company receives no response from law enforcement after the 7th full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

Company will delay notification to customers or the public upon request of the FBI or USSS. If the Company CPNI Compliance Officer believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; Company still may not notify customers sooner unless given clearance to do so from both the USSS and the FBI.

IV. RECORD RETENTION

The Company CPNI Compliance Officer is responsible for assuring that Company maintains for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Company maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties or where third parties were allowed access to CPNI (i.e., pursuant to a valid request from law enforcement, court order or other appropriate authority). If Company later begins to use CPNI for marketing, it will also keep a record for a period of at least one year, of supervisory review of marketing that proposes to use CPNI or to request customer approval to use or disclose CPNI, its sales and marketing campaigns that use its customers' CPNI, including a description of each campaign, the specific CPNI that was used in the campaign, and the products and services offered as a part of the campaign, and records associated with customers' approval or non-approval to use CPNI.

Company maintains a record of all customer complaints related to their handling of CPNI, and records of the Company's handling of such complaints, for at least two years. The CPNI Compliance Officer will assure that all complaints are reviewed and that the Company considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

Company will have an authorized corporate officer, as an agent of the Company, sign a compliance certificate on an annual basis stating that the officer has personal

knowledge that Company has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC Enforcement Bureau in EB Docket No. 06-36 by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how Company's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. Confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

V. TRAINING

Company employees must use a unique login and password to obtain access to databases that include CPNI. All employees with such access to CPNI receive a summary of Company's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties